REMARKS/ARGUMENTS

Reconsideration and withdrawal of the rejection of the application are respectfully requested in view of the amendments and remarks herewith, which place the application into condition for allowance. The present amendment is being made to facilitate prosecution of the application.

I. STATUS OF THE CLAIMS AND FORMAL MATTERS

Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 are pending and are hereby amended. Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 are independent. No new matter has been introduced. Support for this amendment can be found throughout the Specification as originally filed and specifically on page 31, lines 12-18. It is submitted that these claims, as originally presented, were in full compliance with the requirements of 35 U.S.C. §112. Changes to claims are not made for the purpose of patentability within the meaning of 35 U.S.C. §101, §102, §103, or §112. Rather, these changes are made simply for clarification and to round out the scope of protection to which Applicants are entitled.

Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25, which were rejected under 35 U.S.C. §112, second paragraph have been amended, thereby obviating the rejection.

II. REJECTIONS UNDER 35 U.S.C. §103(a)

Claims 1-3, 5-8, 10-13, 15-18, 20-23, and 25 were rejected under 35 U.S.C. §103(a) as allegedly unpatentable over U.S. Patent No. 6,636,968 to Rosner, et al. (hereinafter, merely "Rosner") in view of "Applied Cryptography" by Schneier (hereinafter, merely "Schneier").

Claim 1 recites, *inter alia*:

"A digital data delivery method...comprising the steps of:

encrypting digital data by said upstream system using an encryption key;

generating a plurality of pieces of key information on the basis of said encryption key, respective pieces of said key information being generated by **dividing said encryption key by a division pattern unique to each of said specific destinations and said division pattern based on the content of said digital data**;" (Emphasis added)

As understood by Applicants, Rosner relates to the encryption of information for distribution to multiple recipients.

As understood by Applicants, Schneier relates to secret splitting, secret sharing and distribution of encryption keys.

Applicants submit that Rosner and Schneier fail to teach or suggest the above-identified features of claim 1. Specifically, there is no teaching or suggestion of generating a plurality of pieces of key information on the basis of said encryption key, respective pieces of said key information being generated by dividing said encryption key by a division pattern unique to each of said specific destinations and said division pattern based on the content of said digital data, as recited in independent claim 1.

The Office Action asserts that "Schneier teaches that when performing the splitting of the key, a random number (division pattern) is generated and used in the splitting, as seen in Section 3.6 Step (1) of Schneier on page 70. As such, it is obvious that each time the key is split, the random number is different." However, the present claims recite dividing the encryption key by a division pattern which is unique to each of the destinations and the division pattern is based on the content of the digital data. Generating a different random number each

time the key is split as taught by Schneier will not generate a division pattern which is unique to the destination.

Further, the Office Action asserts that "according to Rosner, the encryption key is periodically updated and the key exchange needs to be performed again. As such, when the key is updated, and the key exchange is performed again, it would be obvious that the new transmitted keys would be split according to the teachings of Schneier and therefore be accorded a new random number (division pattern). As such, the new key would be used to encrypt a new set of content, and as such the random pattern would have "varied" between previous content and the new content." However, as noted above, the encryption key is updated periodically. The same key and thus the same division pattern will be used between updates. Thus, varying content can be encrypted using the encryption key and thus the same division pattern. Therefore, the division pattern does not vary according to the content of the data.

Therefore, Applicants submit that independent claim 1 is patentable.

For reasons similar to, or somewhat similar to, those described above with regard to independent claim 1, independent claims 2, 3, 5-8, 10-13, 15-18, 20-23, and 25 are also believed to be patentable.

CONCLUSION

In the event the Examiner disagrees with any of statements appearing above with respect to the disclosure in the cited reference or references, it is respectfully requested that the Examiner specifically indicate those portion or portions of the reference or references providing the basis for a contrary view.

Please charge any additional fees that may be needed, and credit any overpayment, to our Deposit Account No. 50-0320.

In view of the foregoing amendments and remarks, it is believed that all of the claims in this application are patentable and Applicants respectfully request early passage to issue of the present application.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By_____
Paul A. Levy
Reg. No. 45,748
(212) 588-0800